(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001352319 A**

(43) Date of publication of application: **21.12.01**

(51) Int. Cl **H04L 9/08**
G06F 1/00
G09C 1/00

(21) Application number: **2000126692**

(22) Date of filing: **23.03.00**

(71) Applicant: **MIYAJI MITSUKO**

(72) Inventor: **MIYAJI MITSUKO**

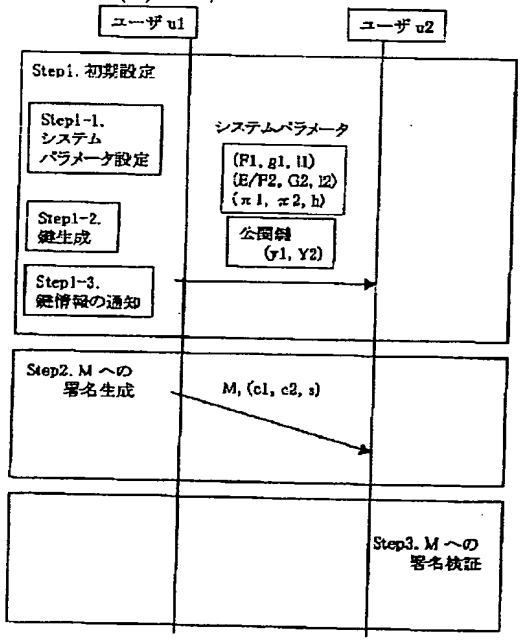
(54) **INTEGRATION SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an integration system that relates to an encryption technology as an information security technology, especially to a key common sharing, encryption and digital signature technology, integrates a factorization problem, a discrete logarithm problem, and a discrete logarithm problem on an elliptic curve having independent security in a way that the respective securities are independent, and can provide a key common share, encryption and signature method having immunity even when one problem is attacked.

SOLUTION: The integration system adopts a key common sharing method that includes an initial setting step (1), a system parameter setting (1-1), a step (1-2) where a key for a user u1 is generated, a notice step (1-3) of key information for the user u1, a step (2) where a signature to data M by the user u1 is generated, and a step (3) where the signature to the data M by a user u2 is verified. Thus, this invention provides the key common share, encryption and signature method that has stiffness against an attack.

COPYRIGHT: (C)2001,JPO



THIS PAGE BLANK (USPTO)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－352319
(P2001－352319A)
(43)公開日　平成13年12月21日(2001.12.21)

(51)Int.Cl.⁷	識別記号	FI		テーマコード(参考)
H04L 9/08		G06F 1/00	370E	5J104
G06F 1/00	370	G09C 1/00	620A	
G09C 1/00	620		620Z	
			640B	
	640	H04L 9/00	601C	

審査請求　未請求　請求項の数18　書面　(全 10 頁)　最終頁に続く

(21)出願番号　特願2000－126692(P2000－126692)

(22)出願日　平成12年３月23日(2000.3.23)

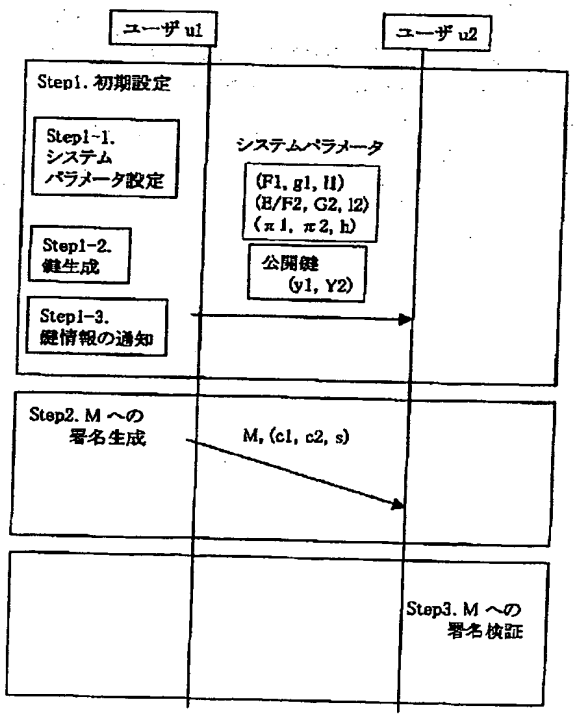
特許法第30条第１項適用申請有り　平成11年９月24日
社団法人電子情報通信学会開催の「電子情報通信学会技術研究報告」において文書をもって発表

(71)出願人　500194647
宮地　充子
石川県能美郡辰口町旭台１－50－Ｅ－41
(72)発明者　宮地　充子
石川県能美郡辰口町旭台１－50－Ｄ－34

Ｆターム(参考)　5J104 AA01 AA09 AA16 EA24 EA28
EA30 EA32 EA33 JA23 JA25
JA27 JA29 LA03 LA05 LA06
NA02 NA12 NA16 NA18

(54)【発明の名称】　統合装置

(57)【要約】
【目的】情報セキュリテイ技術としての暗号技術に関するものであり，特に，複数の安全性の仮定を用いて実現する鍵共有，暗号及びデジタル署名技術に関するものであり，独立な安全性をもつ素因数分解問題，離散対数問題、楕円曲線上の離散対数問題等の問題を互いの安全性が独立であるように統合し，一つの問題が攻撃されても耐用可能な鍵共有，暗号，署名方法を提供することを目的とする．
【構成】
（１）初期設定
（１—１）システムパラメータ設定
（１—２）ユーザｕ１の鍵生成
（１—３）ユーザｕ１の鍵情報の通知
（２）ユーザｕ１によるデータＭへの署名生成
（３）ユーザｕ２によるデータＭへの署名検証
の各ステップを含む鍵共有方法を用いた統合装置．
【効果】攻撃に対する頑強性をもつ鍵共有，暗号及び署名方式を与える．



【特許請求の範囲】

【請求項１】Ｆ１，Ｆ２をともに乗算が定義される有限群とし，ｇ１，ｇ２をそれぞれ有限群Ｆ１，Ｆ２の元とし，ｇ１，ｇ２は位数をそれぞれｌ１，ｌ２としてもつ有限群Ｆ１，Ｆ２を用い、

ユーザｕ１とｕ２の初期設定は，ユーザｕ１は０＜ｘ１＜ｌ１となる整数ｘ１を生成するステップと，生成したｘ１をｕ１の秘密鍵とし，秘密鍵ｘ１に対して，有限群Ｆ１上でｙ１＝ｇ１＾（ｘ１）を求めるステップと，求めたｙ１を公開鍵とし，公開鍵ｙ１とシステムパラメータである有限群Ｆ１，元ｇ１，位数ｌ１をユーザｕ２に通知するステップと，ユーザｕ２は０＜ｘ２＜ｌ２となる整数ｘ２を生成するステップと，生成したｘ２をｕ２の秘密鍵とし，秘密鍵ｘ２に対して，有限群Ｆ２上でｙ２＝ｇ２＾（ｘ２）を求めるステップと，求めたｙ２を公開鍵とし，公開鍵ｙ２とシステムパラメータである有限群Ｆ２，元ｇ２，位数ｌ２をユーザｕ１に通知するステップとからなり，ユーザｕ１とユーザｕ２との鍵共有は、，ユーザｕ１は０＜ｋ１＜ｌ２となる乱数ｋ１を生成するステップと，生成したｋ１を用いて，有限群Ｆ２上でｒ１＝ｇ２＾（ｋ１）を求めるステップと，その出力ｒ１をユーザｕ２に送信するステップと，ユーザｕ２は０＜ｋ２＜ｌ１となる乱数ｋ２を生成するステップと，生成したｋ２を用いて，有限群Ｆ１上でｒ２＝ｇ１＾（ｋ２）を求めるステップと，その出力ｒ２をユーザｕ１に送信するステップと，ユーザｕ１はユーザｕ２より受信したｒ２とｕ２の公開鍵ｙ２及び自分の秘密鍵ｘ１及び乱数ｋ１を用いて，

Ｋ＝（ｒ２＾（ｘ１），ｙ２＾（ｋ１））＝（ｇ１＾（ｘ１×ｋ２），ｇ２＾（ｋ１×ｘ２））∈Ｆ１×Ｆ２

を求め、その出力Ｋを秘密の共有鍵とするステップと、

ユーザｕ２はユーザｕ１より受信したｒ１とｕ１の公開鍵ｙ１及び自分の秘密鍵ｘ２及び乱数ｋ２を用いて，

Ｋ＝（ｙ１＾（ｋ２），ｒ１＾（ｘ２））＝（ｇ１＾（ｘ１×ｋ２），ｇ２＾（ｋ１×ｘ２））∈Ｆ１×Ｆ２

を求め，その出力Ｋを秘密の共有鍵とするステップとからなり、

ユーザｕ１とユーザｕ２がそれぞれのシステムパラメータＦ１，ｇ１，ｌ１及びＦ２，ｇ２，ｌ２を独立に生成し、互いのシステムパラメータを用いて構成した秘密鍵ｘ１，ｘ２を対等に関与させることで鍵Ｋを共有することを特徴とする鍵共有方法．

【請求項２】請求項１記載の鍵共有法を適用した鍵共有装置。

【請求項３】請求項１記載の鍵共有方法を実行するプログラムを記憶した記録媒体。

【請求項４】請求項１記載の有限群Ｆ１，Ｆ２を有限体とすることを特徴とする鍵共有法．

【請求項５】請求項１記載の有限群Ｆ１，Ｆ２を有限体上の楕円曲線Ｅ１（Ｆ１），Ｅ２（Ｆ２）とすることを特徴とする鍵共有法．

【請求項６】請求項１記載の有限群Ｆ１，Ｆ２を有限体，有限体上の楕円曲線Ｆ１，Ｅ２（Ｆ２）とすることを特徴とする鍵共有法．

【請求項７】Ｆ１，Ｆ２を有限群とし，ｇ１，ｇ２をそれぞれ有限群Ｆ１，Ｆ２の元とし，ｇ１，ｇ２の位数をそれぞれｌ１，ｌ２とし，有限群Ｆ１，Ｆ２の演算をともに乗法的に表し，有限群Ｆ１，Ｆ２の元を整数に変換する写像をそれぞれπ１，π２とし，有限群Ｆ１，Ｆ２，元ｇ１，ｇ２，位数ｌ１，ｌ２を格納するメモリ部を有し，有限群Ｆ１，Ｆ２の元を入力とし，そのπ１，π２による出力を計算する演算部を有し，ユーザｕ１は０＜ｘ１＜ｌ１となる整数ｘ１及び０＜ｘ２＜ｌ２となる整数ｘ２を秘密鍵として格納するメモリ部を有し，秘密鍵ｘ１に対して，有限群Ｆ１上の演算でｙ１＝ｇ１＾（ｘ１）を求める演算部と，秘密鍵ｘ２に対して，有限群Ｆ２上の演算でｙ２＝ｇ２＾（ｘ２）を求める演算部を有し、それぞれの出力ｙ１，ｙ２を公開鍵とし，公開鍵ｙ１，ｙ２とシステムパラメータである有限群Ｆ１，Ｆ２，元ｇ１，ｇ２，位数ｌ１，ｌ２，写像π１，π２を他ユーザに通知する通信部を有し，ユーザｕ１に対して秘密にデータＭを送信したいユーザは，０＜ｋ１＜ｌ１及び０＜ｋ２＜ｌ２となる乱数ｋ１，ｋ２を生成し，これを格納するメモリ部を有し，有限群Ｆ１上でｒ１＝ｇ１＾（ｋ１），ｃ１＝ｙ１＾（ｋ１）を，有限群Ｆ２上でｒ２＝ｇ２＾（ｋ２），ｃ２＝ｙ２＾（ｋ２）を求め，

ｃ＝π１（ｃ１）（＋）π２（ｃ２）（＋）Ｍ

を求める演算部を有し，ここで（＋）はビット毎の排他的論理和を表し，その出力（ｒ１，ｒ２，ｃ）をデータＭに対する暗号文Ｍとし，ユーザｕ１に送信する通信部を有し，暗号文（ｒ１，ｒ２，ｃ）を受信したユーザｕ１は，秘密鍵ｘ１，ｘ２を用いて，

Ｍ＝π１（ｒ１＾（ｘ１））（＋）π２（ｒ２＾（ｘ２））（＋）ｃ

を求める演算部を有し，その出力として復号文Ｍを入手し，ユーザｕ１がＦ１に基づく離散対数問題とＦ２に基づく離散対数問題を対等に関与させて暗号化・復号化を行うことを特徴とする暗号化方法．

【請求項８】請求項７記載の暗号化方法を適用した暗号装置。

【請求項９】請求項７記載の方法を実行するプログラムを記憶した記録媒体。

【請求項１０】請求項７記載の有限群Ｆ１，Ｆ２を有限体とすることを特徴とする暗号化方法

【請求項１１】請求項７記載の有限群Ｆ１，Ｆ２を有限体上の楕円曲線Ｅ１（Ｆ１），Ｅ２（Ｆ２）とすることを特徴とする暗号化方法．

【請求項１２】請求項７記載の有限群Ｆ１，Ｆ２を有限体，有限体上の楕円曲線Ｆ１，Ｅ２（Ｆ２）とすること

を特徴とする暗号化方法.

【請求項１３】Ｆ１，Ｆ２を有限群とし，ｇ１，ｇ２をそれぞれ有限群Ｆ１，Ｆ２の元とし，ｇ１，ｇ２の位数をそれぞれｌ１，ｌ２とし，ここでｌ１とｌ２は互いに素とし，有限群Ｆ１，Ｆ２の演算をともに乗法的に表し，有限群Ｆ１，Ｆ２の元を整数に変換する写像をそれぞれπ１，π２とし，任意のビット数の整数の元をある固定されたビット数に写像するハッシュ関数をｈとし，有限群Ｆ１，Ｆ２，元ｇ１，ｇ２，位数ｌ１，ｌ２を格納するメモリ部を有し，有限群Ｆ１，Ｆ２の元を入力とし，そのπ１，π２による出力を計算する演算部と任意のビット数の整数の元を入力とし，そのｈによる出力を計算する演算部を有し，ユーザｕ１は０＜ｘ１＜ｌ１となる整数ｘ１及び０＜ｘ２＜ｌ２となる整数ｘ２を秘密鍵として格納するメモリ部を有し，秘密鍵ｘ１に対して，有限群Ｆ１上の演算でｙ１＝ｇ１＾（ｘ１）を求める演算部と，秘密鍵ｘ２に対して，有限群Ｆ２上の演算でｙ２＝ｇ２＾（ｘ２）を求める演算部を有し，それぞれの出力ｙ１，ｙ２を公開鍵とし，公開鍵ｙ１，ｙ２とシステムパラメータである有限群Ｆ１，Ｆ２，元ｇ１，ｇ２，位数ｌ１，ｌ２，写像π１，π２，ｈを他ユーザに通知する通信部を有し，ユーザｕ１が、データＭに対してディジタル署名を施してユーザｕ２に送信したいとき、０＜ｋ１＜ｌ１及び０＜ｋ２＜ｌ２となる乱数ｋ１，ｋ２を生成し，これを格納するメモリ部を有し，データＭに対しｅ＝ｈ（Ｍ）を求め，有限群Ｆ１上でｒ１＝ｇ１＾（ｋ１）を，有限群Ｆ２上でｒ２＝ｇ２＾（ｋ２）を求め，次に、ｃ１＝π１（ｒ１）（ｍｏｄ　ｌ１），ｃ２＝π２（ｒ２）（ｍｏｄ　ｌ２）を求め，

ｓ１＝ｋ１＾（—１）（ｅ＋ｘ１ｃ１）（ｍｏｄ　ｌ１）

ｓ２＝ｋ２＾（—１）（ｅ＋ｘ２ｃ２）（ｍｏｄ　ｌ２）

となる０＜ｓ１＜ｌ１—１，０＜ｓ２＜ｌ２—１を求め，

０＜ｓ＜ｌ１×ｌ２でかつｓ＝ｓ１（ｍｏｄ　ｌ１），

ｓ＝ｓ２（ｍｏｄｌ２）

となるｓを求める演算部を有し，その出力（ｃ１，ｃ２，ｓ）をデータＭに対する署名文としてユーザｕ２に送信する通信部を有し，署名文（ｃ１，ｃ２，ｓ）を受信したユーザｕ２は，ユーザｕ１の公開鍵及びシステムパラメータを用いて，

ｅ’＝ｈ（Ｍ），

ｓ１’＝ｓ（ｍｏｄ　ｌ１），ｓ２’＝ｓ（ｍｏｄ　ｌ２），

Ｆ１上でｒ１’＝ｇ１＾（ｅ’／ｓ１’）ｙ１＾（ｃ１／ｓ１），

Ｆ２上でｒ２’＝ｇ２＾（ｅ’／ｓ２’）ｙ２＾（ｃ２／ｓ２），

ｃ１’＝π１（ｒ１’），ｃ２’＝π２（ｒ２’）

を求める演算部と，

ｃ１＝ｃ１’（ｍｏｄ　ｌ１），ｃ２＝ｃ２’（ｍｏｄ　ｌ２）

であるか判定する判定部を有し，判定結果により署名を検証する，ユーザｕ１がＦ１に基づく離散対数問題とＦ２に基づく離散対数問題を対等に関与させて署名生成，検証を行うことを特徴とする署名方法.

【請求項１４】請求項１３記載の署名方法を適用した署名装置。

【請求項１５】請求項１３記載の方法を実行するプログラムを記憶した記録媒体。

【請求項１６】請求項１３記載の有限群Ｆ１，Ｆ２を有限体とすることを特徴とする署名方法.

【請求項１７】請求項１３記載の有限群Ｆ１，Ｆ２を有限体上の楕円曲線Ｅ１（Ｆ１），Ｅ２（Ｆ２）とすることを特徴とする署名方法.

【請求項１８】請求項１３記載の有限群Ｆ１，Ｆ２を有限体，有限体上の楕円曲線Ｆ１，Ｅ２（Ｆ２）とすることを特徴とする署名方法.

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は情報セキュリテイ技術としての暗号技術に関するものであり，特に，複数の安全性の仮定を用いて実現する鍵共有，暗号及びデジタル署名技術に関するものである.

【０００２】

【従来の技術】秘密通信方式とは，特定の通信相手以外に通信内容を漏らすことなく通信を行なう方式である．またデジタル署名方式とは，通信相手に通信内容の正当性を示したり，本人であることを証明する通信方式である．この署名方式には公開鍵暗号とよばれる暗号方式を用いる．公開鍵暗号は通信相手が多数の時，通信相手ごとに異なる暗号鍵を容易に管理するための方式であり，多数の通信相手と通信を行なうのに不可欠な基盤技術である．簡単に説明すると，これは暗号化鍵と復号化鍵が異なり，復号化鍵は秘密にするが，暗号化鍵を公開する方式である．この公開鍵暗号の安全性の根拠に用いられるものに離散対数問題がある．離散対数問題には代表的に，有限体上定義されるもの及び楕円曲線上定義されるものがある．これはニイルコブリッツ著 ”ア コウス イン ナンバア セオリイ アンド クリプトグラヒイ”（Ｎｅａｌ Ｋｏｂｌｉｔｚ，″Ａ Ｃｏｕｒｓｅ ｉｎＮｕｍｂｅｒ ｔｈｅｏｒｙ ａｎｄ Ｃｒｙｐｔｏｇｒａｐｈｙ″，Ｓｐｉｎｇｅｒ—Ｖｅｒｌａｇ，１９８７）に詳しく述べられている．楕円曲線上の離散対数問題を以下に述べる.

【０００３】楕円曲線上の離散対数問題

Ｅ（Ｆｐ）を有限体Ｆｐ上定義された楕円曲線Ｅとし，Ｅの位数が大きな素数で割れる元Ｇをベースポイントとする．このとき，Ｅの与えられた元Ｙに対して，

Ｙ＝ｘＧ
となる整数ｘが存在するならばｘを求めよ．
【０００４】以下に上記楕円曲線上の離散対数問題を応用したＤＳＡ署名をまず述べる。
従来例１
図３ は従来例である楕円曲線上のＤＳＡ署名方式の構成をしめすものである。以下同図を参照しながら従来例の手順を説明する。
（１）初期設定
有限体Ｆ上の楕円曲線をＥとし、その素数位数ｑの元をＧ，楕円曲線の元Ｅ（Ｆ）を整数に対応させる写像をπ，任意長の整数をある固定された長さに写すハッシュ関数をｈとする。ユーザｕ１の公開鍵をＹａ＝ｘａＧとし、秘密鍵をｘａとする。ｕ１の公開鍵とともに，楕円曲線Ｅ／Ｆ，ベースポイントＧ，写像π，ｈをシステムパラメータとして公開する。
【０００５】（２）メッセージＭに対するユーザｕ１の署名生成
１．ｅ＝ｈ（Ｍ）を計算する．
２．乱数０＜ｋ＜１を生成する。
３．Ｒ１＝ｋＧ，ｃ１＝π（Ｒ１）（ｍｏｄ　ｑ），
ｓ＝ｋ＾（—１）（ｅ　＋ｃ１×ｘａ）（ｍｏｄ　ｑ）
を計算する．ここでｃ１＝０あるいはｓ＝０であればもう一度，２に戻ってｋをとり直す．
４．（ｃ１、ｓ）を署名としてＭとともに送信する。
【０００６】（３）署名検証
１．ｅ＝ｈ（Ｍ）を計算する．
２．ｃ１＝０あるいは　ｓ＝０であれば，ＮＧを出力．
３．Ｒ１’＝ｅ／ｓＧ＋ｃ１／ｓ　Ｙ，
ｃ１’＝π（Ｒ１’）
を計算する．
４．ｃ１＝ｃ１’（ｍｏｄ　ｑ）であればＯＫを出力し，そうでないときはＮＧを出力する．
【０００７】上記従来例１では，一つの楕円曲線　Ｅの離散対数問題に安全性に依存している．このため，利用している楕円曲線Ｅ上の離散対数問題が攻撃できると，ユーザの署名方式の安全性が損なわれることになる．ユーザがクライアントの位置付けであれば，被害は小さいかもしれないが，例えばサーバであったり公開鍵証明書発行局であるなど公的な位置付けの機関の方式が解読されると被害が非常に大きい．
【０００８】ところが，楕円曲線の離散対数問題では，特定の楕円曲線に対して適用可能な攻撃が提案されるなど，一つの楕円曲線に依存したシステムの安全性が指摘されている．これについては以下の論文が詳しい．
Ａ．Ｍｅｎｅｚｅｓ，Ｔ．Ｏｋａｍｏｔｏ　ａｎｄ　Ｓ．Ｖａｎｓｔｏｎｅ，``Ｒｅｄｕｃｉｎｇ　ｅｌｌｉｐｔｉｃ　ｃｕｒｖｅ　ｌｏｇａｒｉｔｈｍｓｔｏ　ｌｏｇａｒｉｔｈｍｓ　ｉｎ　ａ　ｆｉｎｉｔｅ　ｆｉｅｌｄ''，ＩＥＥＥ　Ｔｒａｎｓａｃｔｉｏｎｓ　ｏｎ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｔｈｅｏｒｙ，３９（１９９３），１６３９—１６４６．
Ｔ．Ｓａｔｏｈ　ａｎｄ　Ｋ．Ａｒａｋｉ，``Ｆｅｒｍａｔ　ｑｕｏｔｉｅｎｔｓ　ａｎｄ　ｔｈｅ　ｐｏｌｙｎｏｍｉａｌ　ｔｉｍｅ　ｄｉｓｃｒｅｔｅ　ｌｏｇ　ａｌｇｏｒｉｔｈｍ　ｆｏｒ　ａｎｏｍａｌｏｕｓ　ｅｌｌｉｐｔｉｃ　ｃｕｒｖｅ''，Ｃｏｍｍｅｎｔａｒｉｉ　Ｍａｔｈ．　Ｕｎｉｖ．　Ｓｔ．Ｐａｕｌｉ．，ｖｏｌ．４７（１９８８），８１—９２．
【０００９】次に有限体上の離散対数問題を利用した鍵共有方式を従来例としてあげる．
従来例２
図４は従来例である有限体上のＤＨ鍵共有方式の構成をしめすものである。以下同図を参照しながら従来例の手順を説明する。
（１）初期設定
有限体Ｆの素数位数ｑの元をｇとする。ユーザｕ１の秘密鍵をｘａ，公開鍵をｙａ＝ｇ＾ｘａとし，ユーザｕ２の秘密鍵をｘｂ，公開鍵をｙｂ＝ｇ＾ｘｂとする．ユーザの公開鍵とともに，有限体Ｆ，ベースポイントｇ，位数ｑをシステムパラメータとして公開する。
【００１０】（２）鍵共有
ユーザｕ１は，
１．乱数０＜ｋａ＜ｑを生成する。
２．有限体Ｆ上で，
ｒ１＝ｇ＾ｋａ
を計算し，ｕ２に送信する．ユーザｕ２は，
３．乱数０＜ｋｂ＜ｑを生成する。
４．有限体Ｆ上で，
ｒ２＝ｇ＾ｋｂ
を計算し，ｕ１に送信する．
ユーザｕ１は，
５．受信したｒ２とｕ２の公開鍵ｙｂと　自分の秘密鍵ｘａ乱数ｋａを用いて，有限体Ｆ上で，
Ｋ＝（ｒ２＾ｘａ，ｙｂ＾ｋａ）＝（ｇ＾（ｋｂ×ｘａ），ｇ＾（ｋａ×ｘｂ））∈Ｆ×Ｆ
を計算し，共有鍵Ｋを得る．ユーザｕ２は，
６．受信したｒ１とｕ１の公開鍵ｙａと自分の秘密鍵ｘｂ乱数ｋｂを用いて，有限体Ｆ上で，
Ｋ＝（ｙａ＾ｋｂ，ｒ１＾ｘｂ）＝（ｇ＾（ｋｂ×ｘａ），ｇ＾（ｋａ×ｘｂ））∈Ｆ×Ｆ
を計算し，共有鍵Ｋを得る．
【００１１】従来例２で見たように，鍵共有を実現したいユーザはともに同じシステムパラメータを共有し，そのシステムパラメータ上で公開鍵と秘密鍵のペアを生成し，共有鍵の安全性も利用した１つのシステムパラメータに依存する．しかしながら，異なるユーザの間で同じシステムパラメータの利用を強制することは，ユーザの利便性を損なう．また，安全性の観点からも従来例１で述べたように，１つのシステムパラメータに依存してい

るので，このパラメータが解読されると両ユーザのシステムパラメータを変更しなければならないといい問題を持つ．

【００１２】

【発明が解決しようとする課題】公開鍵暗号を用いた暗号方式，鍵共有方式，署名方式では，攻撃に対して，可能な限り強力に構成することが必須である．従来例の暗号方式，鍵共有方式，署名方式においては，安全性の根拠を離散対数問題や素因数分解という一つの問題（システムパラメータと呼ばれる）に帰着している．しかしながら，この方法では，安全性を帰着している問題が攻撃された場合，その方式で構成されたすべてのデータが攻撃されることになる．特に，近年楕円曲線上の離散対数問題の攻撃に見られるように，特定の楕円曲線上の離散対数問題が攻撃されるなど，１つの方式に安全性を帰着させたシステムは，攻撃に対して非常に弱いという欠点がある．

【００１３】また，ユーザが自由にシステムパラメータを生成し決定できる方が、より汎用的でかつ安全な方式を与える。しかし鍵共有方式においては、従来例２で見たように、同じシステムパラメータ上での計算を要求するので、事前に同じシステムパラメータ上で公開鍵、秘密鍵のペアを生成する必要がある。また、上述と同様に、利用したシステムパラメータに基づく問題が攻撃されると、安全性が損なわれるという問題がある。

【００１４】本発明は，この従来例における問題点を鑑みて行なわれたもので，独立な安全性をもつ素因数分解、離散対数問題、楕円曲線上の離散対数問題などのシステムパラメータを互いの安全性が独立であるように統合し，攻撃されても耐用可能な鍵共有，暗号，署名方法を提供することを目的とする．

【００１５】

【課題を解決するための手段】本発明は上述の問題点を解決するため，請求項１では、Ｆ１，Ｆ２をともに乗算が定義される有限群とし，ｇ１，ｇ２をそれぞれ有限群Ｆ１，Ｆ２の元とし，ｇ１，ｇ２は位数をそれぞれｌ１，ｌ２としてもつ有限群Ｆ１，Ｆ２を用い、ユーザｕ１とｕ２の初期設定は，ユーザｕ１は０＜ｘ１＜ｌ１となる整数ｘ１を生成するステップと，生成したｘ１をｕ１の秘密鍵とし，秘密鍵ｘ１に対して，有限群Ｆ１上でｙ１＝ｇ１＾（ｘ１）を求めるステップと，求めたｙ１を公開鍵とし，公開鍵ｙ１とシステムパラメータである有限群Ｆ１，元ｇ１，位数ｌ１をユーザｕ２に通知するステップと，ユーザｕ２は０＜ｘ２＜ｌ２となる整数ｘ２を生成するステップと，生成したｘ２をｕ２の秘密鍵とし，秘密鍵ｘ２に対して，有限群Ｆ２上でｙ２＝ｇ２＾（ｘ２）を求めるステップと，求めたｙ２を公開鍵とし，公開鍵ｙ２とシステムパラメータである有限群Ｆ２，元ｇ２，位数ｌ２をユーザｕ１に通知するステップとからなり，ユーザｕ１とユーザｕ２との鍵共有は、，ユーザｕ１は０＜ｋ１＜ｌ２となる乱数ｋ１を生成するステップと，生成したｋ１を用いて，有限群Ｆ２上でｒ１＝ｇ２＾（ｋ１）を求めるステップと，その出力ｒ１をユーザｕ２に送信するステップと，ユーザｕ２は０＜ｋ２＜ｌ１となる乱数ｋ２を生成するステップと，生成したｋ２を用いて，有限群Ｆ１上でｒ２＝ｇ１＾（ｋ２）を求めるステップと，その出力ｒ２をユーザｕ１に送信するステップと，ユーザｕ１はユーザｕ２より受信したｒ２とｕ２の公開鍵ｙ２及び自分の秘密鍵ｘ１及び乱数ｋ１を用いて，

Ｋ＝（ｒ２＾（ｘ１），ｙ２＾（ｋ１））＝（ｇ１＾（ｘ１×ｋ２），ｇ２＾（ｋ１×ｘ２））∈Ｆ１×Ｆ２

を求め、その出力Ｋを秘密の共有鍵とするステップと、ユーザｕ２はユーザｕ１より受信したｒ１とｕ１の公開鍵ｙ１及び自分の秘密鍵ｘ２及び乱数ｋ２を用いて，

Ｋ＝（ｙ１＾（ｋ２），ｒ１＾（ｘ２））＝（ｇ１＾（ｘ１×ｋ２），ｇ２＾（ｋ１×ｘ２））∈Ｆ１×Ｆ２

を求め，その出力Ｋを秘密の共有鍵とするステップとからなり、ユーザｕ１とユーザｕ２がそれぞれのシステムパラメータＦ１，ｇ１，ｌ１及びＦ２，ｇ２，ｌ２を独立に生成し、互いのシステムパラメータを用いて構成した秘密鍵ｘ１，ｘ２を対等に関与させることで鍵Ｋを共有することを特徴とする鍵共有方法としている．

【００１６】請求項２では，請求項１記載の鍵共有法を適用した鍵共有装置としている．

【００１７】請求項３では，請求項１記載の鍵共有方法を実行するプログラムを記憶した記録媒体としている．

【００１８】請求項４では，請求項１記載の有限群Ｆ１，Ｆ２を有限体とすることを特徴とする鍵共有法としている．

【００１９】請求項５では，請求項１記載の有限群Ｆ１，Ｆ２を有限体上の楕円曲線Ｅ１（Ｆ１），Ｅ２（Ｆ２）とすることを特徴とする鍵共有法としている．

【００２０】請求項６では，請求項１記載の有限群Ｆ１，Ｆ２を有限体，有限体上の楕円曲線Ｆ１，Ｅ２（Ｆ２）とすることを特徴とする鍵共有法としている．

【００２１】請求項７では，Ｆ１，Ｆ２を有限群とし，ｇ１，ｇ２をそれぞれ有限群Ｆ１，Ｆ２の元とし，ｇ１，ｇ２の位数をそれぞれｌ１，ｌ２とし，有限群Ｆ１，Ｆ２の演算をともに乗法的に表し，有限群Ｆ１，Ｆ２の元を整数に変換する写像をそれぞれπ１，π２とし，有限群Ｆ１，Ｆ２，元ｇ１，ｇ２，位数ｌ１，ｌ２を格納するメモリ部を有し，有限群Ｆ１，Ｆ２の元を入力とし，そのπ１，π２による出力を計算する演算部を有し，ユーザｕ１は０＜ｘ１＜ｌ１となる整数ｘ１及び０＜ｘ２＜ｌ２となる整数ｘ２を秘密鍵として格納するメモリ部を有し，秘密鍵ｘ１に対して，有限群Ｆ１上の演算でｙ１＝ｇ１＾（ｘ１）を求める演算部と，秘密鍵ｘ２に対して，有限群Ｆ２上の演算でｙ２＝ｇ２＾（ｘ２）を求める演算部を有し、それぞれの出力ｙ１，ｙ２

を公開鍵とし，公開鍵ｙ１，ｙ２とシステムパラメータである有限群Ｆ１，Ｆ２，元ｇ１，ｇ２，位数ｌ１，ｌ２，写像π１，π２を他ユーザに通知する通信部を有し，ユーザｕ１に対して秘密にデータＭを送信したいユーザは，０＜ｋ１＜ｌ１及び０＜ｋ２＜ｌ２となる乱数ｋ１，ｋ２を生成し，これを格納するメモリ部を有し，有限群Ｆ１上でｒ１＝ｇ１＾（ｋ１），ｃ１＝ｙ１＾（ｋ１）を，有限群Ｆ２上でｒ２＝ｇ２＾（ｋ２），ｃ２＝ｙ２＾（ｋ２）を求め，

ｃ＝π１（ｃ１）（＋）π２（ｃ２）（＋）Ｍ

を求める演算部を有し，ここで（＋）はビット毎の排他的論理和を表し，その出力（ｒ１，ｒ２，ｃ）をデータＭに対する暗号文Ｍとし，ユーザｕ１に送信する通信部を有し，暗号文（ｒ１，ｒ２，ｃ）を受信したユーザｕ１は，秘密鍵ｘ１，ｘ２を用いて，

Ｍ＝π１（ｒ１＾（ｘ１））（＋）π２（ｒ２＾（ｘ２））（＋）ｃ

を求める演算部を有し，その出力として復号文Ｍを入手し，ユーザｕ１がＦ１に基づく離散対数問題とＦ２に基づく離散対数問題を対等に関与させて暗号化・復号化を行うことを特徴とする暗号化方法としている．

【００２２】請求項８では，請求項７記載の暗号化方法を適用した暗号装置としている．

【００２３】請求項９では，請求項７記載の方法を実行するプログラムを記憶した記録媒体としている．

【００２４】請求項１０では，請求項７記載の有限群Ｆ１，Ｆ２を有限体とすることを特徴とする暗号化方法としている．

【００２５】請求項１１では，請求項７記載の有限群Ｆ１，Ｆ２を有限体上の楕円曲線Ｅ１（Ｆ１），Ｅ２（Ｆ２）とすることを特徴とする暗号化方法としている．

【００２６】請求項１２では，請求項７記載の有限群Ｆ１，Ｆ２を有限体，有限体上の楕円曲線Ｆ１，Ｅ２（Ｆ２）とすることを特徴とする暗号化方法としている．

【００２７】請求項１３では，Ｆ１，Ｆ２を有限群とし，ｇ１，ｇ２をそれぞれ有限群Ｆ１，Ｆ２の元とし，ｇ１，ｇ２の位数をそれぞれｌ１，ｌ２とし，ここでｌ１とｌ２は互いに素とし，有限群Ｆ１，Ｆ２の演算をともに乗法的に表し，有限群Ｆ１，Ｆ２の元を整数に変換する写像をそれぞれπ１，π２とし，任意のビット数の整数の元をある固定されたビット数に写像するハッシュ関数をｈとし，有限群Ｆ１，Ｆ２，元ｇ１，ｇ２，位数ｌ１，ｌ２を格納するメモリ部を有し，有限群Ｆ１，Ｆ２の元を入力とし，そのπ１，π２による出力を計算する演算部と任意のビット数の整数の元を入力とし，そのｈによる出力を計算する演算部を有し，ユーザｕ１は０＜ｘ１＜ｌ１となる整数ｘ１及び０＜ｘ２＜ｌ２となる整数ｘ２を秘密鍵として格納するメモリ部を有し，秘密鍵ｘ１に対して，有限群Ｆ１上の演算でｙ１＝ｇ１＾（ｘ１）を求める演算部と，秘密鍵ｘ２に対して，有限群Ｆ２上の演算でｙ２＝ｇ２＾（ｘ２）を求める演算部を有し、それぞれの出力ｙ１，ｙ２を公開鍵とし，公開鍵ｙ１，ｙ２とシステムパラメータである有限群Ｆ１，Ｆ２，元ｇ１，ｇ２，位数ｌ１，ｌ２，写像π１，π２，ｈを他ユーザに通知する通信部を有し，ユーザｕ１が、データＭに対してディジタル署名を施してユーザｕ２に送信したいとき、０＜ｋ１＜ｌ１及び０＜ｋ２＜ｌ２となる乱数ｋ１，ｋ２を生成し，これを格納するメモリ部を有し，データＭに対しｅ＝ｈ（Ｍ）を求め，有限群Ｆ１上でｒ１＝ｇ１＾（ｋ１）を，有限群Ｆ２上でｒ２＝ｇ２＾（ｋ２）を求め，次に、ｃ１＝π１（ｒ１）（ｍｏｄ　ｌ１），ｃ２＝π２（ｒ２）（ｍｏｄ　ｌ２）を求め，

ｓ１＝ｋ１＾（—１）（ｅ＋ｘ１ｃ１）（ｍｏｄ　ｌ１）

ｓ２＝ｋ２＾（—１）（ｅ＋ｘ２ｃ２）（ｍｏｄ　ｌ２）

となる０＜ｓ１＜ｌ１—１，０＜ｓ２＜ｌ２—１を求め，

０＜ｓ＜ｌ１×ｌ２でかつｓ＝ｓ１（ｍｏｄ　ｌ１），ｓ＝ｓ２（ｍｏｄｌ２）

となるｓを求める演算部を有し，その出力（ｃ１，ｃ２，ｓ）をデータＭに対する署名文としてユーザｕ２に送信する通信部を有し，署名文（ｃ１，ｃ２，ｓ）を受信したユーザｕ２は，ユーザｕ１の公開鍵及びシステムパラメータを用いて，

ｅ’＝ｈ（Ｍ），

ｓ１’＝ｓ（ｍｏｄ　ｌ１），ｓ２’＝ｓ（ｍｏｄ　ｌ２），

Ｆ１上でｒ１’＝ｇ１＾（ｅ’／ｓ１’）ｙ１＾（ｃ１／ｓ１），

Ｆ２上でｒ２’＝ｇ２＾（ｅ’／ｓ２’）ｙ２＾（ｃ２／ｓ２），

ｃ１’＝π１（ｒ１’），ｃ２’＝π２（ｒ２’）

を求める演算部と，

ｃ１＝ｃ１’（ｍｏｄ　ｌ１），ｃ２＝ｃ２’（ｍｏｄ　ｌ２）

であるか判定する判定部を有し，判定結果により署名を検証する，ユーザｕ１がＦ１に基づく離散対数問題とＦ２に基づく離散対数問題を対等に関与させて署名生成，検証を行うことを特徴とする署名方法としている．

【００２８】請求項１４では，請求項１３記載の署名方法を適用した署名装置としている．

【００２９】請求項１５では，請求項１３記載の方法を実行するプログラムを記憶した記録媒体としている．

【００３０】請求項１６では，請求項１３記載の有限群Ｆ１，Ｆ２を有限体とすることを特徴とする署名方法としている．

【００３１】請求項１７では，請求項１３記載の有限群Ｆ１，Ｆ２を有限体上の楕円曲線Ｅ１（Ｆ１），Ｅ２

（Ｆ２）とすることを特徴とする署名方法としている．

【００３２】請求項１８では，請求項１３記載の有限群Ｆ１，Ｆ２を有限体，有限体上の楕円曲線Ｆ１，Ｅ２（Ｆ２）とすることを特徴とする署名方法としている．

【００３３】

【実施例１】図１は，有限体上の離散対数問題と楕円曲線上の離散対数問題を用いた署名方法を示すものである．以下同図を参照しながら署名方法を説明する。

Ｓｔｅｐ　１．初期設定

ｓｔｅｐ　１—１．システムパラメータ設定

Ｆ１，Ｅ／Ｆ２を有限体，有限体上の楕円曲線，ｇ１，Ｇ２をそれぞれＦ１，Ｅ（Ｆ２）の元，ｇ１，Ｇ２の位数をそれぞれｌ１，ｌ２，ここでｌ１とｌ２は互いに素とし，有限体Ｆ１，楕円曲線Ｅ（Ｆ２）の元を整数に変換する写像をそれぞれπ１，π２，任意のビット数の整数の元をある固定されたビット数に写像するハッシュ関数ｈを設定する．

ｓｔｅｐ　１—２．ユーザｕ１の鍵生成

ユーザｕ１は０＜ｘ１＜ｌ１となる整数ｘ１及び０＜ｘ２＜ｌ２となる

整数ｘ２を秘密鍵として格納し，秘密鍵ｘ１に対して，Ｆ１上でｙ１＝ｇ１＾（ｘ１），秘密鍵ｘ２に対して，Ｅ（Ｆ２）上でＹ２＝（ｘ２）Ｇ２を求め，それぞれの出力ｙ１，Ｙ２を公開鍵とする．

ｓｔｅｐ　１—３．ユーザｕ１の鍵情報の通知

公開鍵ｙ１，Ｙ２とシステムパラメータであるＦ１，Ｅ（Ｆ２），ｇ１，Ｇ２，ｌ１，ｌ２，π１，π２，ｈを他ユーザに通知する．

【００３４】Ｓｔｅｐ　２．ユーザｕ１によるデータＭへの署名生成

０＜ｋ１＜ｌ１及び０＜ｋ２＜ｌ２となる乱数ｋ１，ｋ２を生成し，データＭに対しｅ＝ｈ（Ｍ）を求め，有限体Ｆ１上でｒ１＝ｇ１＾（ｋ１）を，楕円曲線Ｅ（Ｆ２）上でＲ２＝（ｋ２）Ｇ２を求め，次に、ｃ１＝π１（ｒ１）（ｍｏｄ　ｌ１），ｃ２＝π２（Ｒ２）（ｍｏｄ　ｌ２）を求め，

ｓ１＝ｋ１＾（—１）（ｅ＋ｘ１ｃ１）（ｍｏｄ　ｌ１）

ｓ２＝ｋ２＾（—１）（ｅ＋ｘ２ｃ２）（ｍｏｄ　ｌ２）

となる０＜ｓ１＜ｌ１—１，０＜ｓ２＜ｌ２—１を求め，

０＜ｓ＜ｌ１×ｌ２でかつｓ＝ｓ１（ｍｏｄ　ｌ１），ｓ＝ｓ２（ｍｏｄｌ２）

となるｓを求める．その出力（ｃ１，ｃ２，ｓ）をデータＭに対する署名文としてユーザｕ２に送信する．

【００３５】Ｓｔｅｐ　３．ユーザｕ２によるデータＭへの署名検証ユーザｕ１の公開鍵及びシステムパラメータを用いて，

ｅ’＝ｈ（Ｍ），

ｓ１’＝ｓ（ｍｏｄ　ｌ１），ｓ２’＝ｓ（ｍｏｄ　ｌ２），

Ｆ１上でｒ１’＝ｇ１＾（ｅ’／ｓ１’）ｙ１＾（ｃ１／ｓ１），

Ｅ（Ｆ２）上でＲ２’＝（ｅ’／ｓ２’）Ｇ２＋（ｃ２／ｓ２）Ｙ２，

ｃ１’＝π１（ｒ１’），ｃ２’＝π２（Ｒ２’）

を求め，

ｃ１＝ｃ１’（ｍｏｄ　ｌ１），ｃ２＝ｃ２’（ｍｏｄ　ｌ２）

ならば，正しい署名と判定し，そうでなければ署名を拒絶する．

【００３６】上記実施例１は、異なる独立な安全性を持つ２つの署名方式を対等に関与させた署名方式となっている．つまり、有限体Ｆ１上の離散対数問題と楕円曲線Ｅ／Ｆ２上の離散対数問題に対して、ｓｔｅｐ１において、それぞれの群上で公開鍵と秘密鍵のペアを生成し、ｓｔｅｐ２において両方の秘密情報を対等に、すなわち主従、あるいは時系列的な順序なく関与させて、署名の生成を行っている。この結果，仮に１つの署名方式の安全性が損なわれても，署名方式の安全性はもう一方の署名方式で保たれることが可能になる．

【００３７】実施例１では，有限体上の離散対数問題と楕円曲線上の離散対数問題の２つを統合した署名方式となっているが，実施例はこれに限定されない．例えばＲＳＡ，有限体上の離散対数問題，楕円曲線上の離散対数問題など，安全性の異なる２つ以上の方式を独立に対等に統合することにより，安全性を強化することも含まれる．また言うまでもなく、本実施例では、ＤＳＡ署名ベースの統合を行っているが、それ以外の署名、ｓｃｈｎｏｒｒ署名、Ｎｙｂｅｒｇ—Ｒｕｅｐｐｅｌ署名など、異なる書名方式の統合も含まれる。

【００３８】

【実施例２】図２は，有限体上の離散対数問題と楕円曲線上の離散対数問題を用いた鍵共有方法を示すものである．以下同図を参照しながら署名方法を説明する。

Ｓｔｅｐ　１．初期設定

Ｓｔｅｐ　１—１．ユーザｕ１の鍵生成

ユーザｕ１は，Ｆ１を有限体，ｇ１をＦ１の元とし，その位数ｌ１に対して，０＜ｘ１＜ｌ１となる整数ｘ１を生成し，Ｆ１上でｙ１＝ｇ１＾（ｘ１）を求め，求めたｙ１を公開鍵，生成したｘ１をｕ１の秘密鍵とし，公開鍵ｙ１とシステムパラメータであるＦ１，元ｇ１，位数ｌ１をユーザｕ２に通知する．

ｓｔｅｐ１—２．ユーザｕ２の鍵生成

ユーザｕ２は，Ｅ（Ｆ２）を有限体上の楕円曲線，Ｇ２をＥ（Ｆ２）の元とし，その位数ｌ２に対し，０＜ｘ２＜ｌ２となる整数ｘ２を生成し，Ｅ（Ｆ２）上でＹ２＝（ｘ２）Ｇ２を求め，求めたＹ２を公開鍵，生成したｘ２をｕ２の秘密鍵とし，公開鍵Ｙ２とシステムパラメー

タであるＥ（Ｆ２），元Ｇ２，位数ｌ２をユーザｕ１に通知する．

【００３９】Ｓｔｅｐ　２．ユーザｕ１とユーザｕ２との鍵共有

ｓｔｅｐ　２—１．ユーザｕ１の処理

ユーザｕ１は０＜ｋ１＜ｌ２となる乱数ｋ１を生成し，Ｅ（Ｆ２）上でＲ１＝（ｋ１）Ｇ２を求め，その出力Ｒ１をユーザｕ２に送信する．

ｓｔｅｐ　２—２．ユーザｕ２の処理

ユーザｕ２は０＜ｋ２＜ｌ１となる乱数ｋ２を生成し，Ｆ１上でｒ２＝ｇ１＾（ｋ２）を求め，その出力ｒ２をユーザｕ１に送信する．

ｓｔｅｐ　２—３．ユーザｕ１の鍵共有処理

ユーザｕ１はユーザｕ２より受信したｒ２とｕ２の公開鍵ｙ２及び自分の秘密鍵ｘ１及び乱数ｋ１を用いて，Ｋ＝（ｒ２＾（ｘ１），（ｋ１）Ｙ２）＝（ｇ１＾（ｘ１×ｋ２），（ｋ１×ｘ２）Ｇ２）∈Ｆ１×Ｅ（Ｆ２）を求め、その出力Ｋを秘密の共有鍵とする．

ｓｔｅｐ　２—４．ユーザｕ２の鍵共有処理

ユーザｕ２はユーザｕ１より受信したｒ１とｕ１の公開鍵ｙ１及び自分の秘密鍵ｘ２及び乱数ｋ２を用いて，Ｋ＝（ｙ１＾（ｋ２），（ｘ２）Ｒ１）＝（ｇ１＾（ｘ１×ｋ２），（ｋ１×ｘ２）Ｇ２）∈Ｆ１×Ｅ（Ｆ２）を求め，その出力Ｋを秘密の共有鍵とする．

【００４０】上記実施例２は、各ユーザが独立な安全性を持つ群を生成し，それらを対等に関与させた鍵共有方法となっている．つまり各ユーザは、それぞれ有限体Ｆ１上の離散対数問題と楕円曲線Ｅ／Ｆ２上の離散対数問題に対して、ｓｔｅｐ１において、各ユーザの利用する群上で公開鍵と秘密鍵のペアを独立に生成し、ｓｔｅｐ２において両方の秘密情報を対等に、すなわち主従、あるいは時系列的な順序なく関与させて、鍵共有を行っている。この結果，各ユーザは、鍵共有を行うユーザ間で、同じシステムパラメータを用いて公開鍵と秘密鍵を生成する必要なく鍵共有が可能になり、ユーザの利便性が図られている。さらに、仮に一方のユーザの方式の安全性が損なわれても，鍵共有方式の安全性はもう一方のユーザの方式で保たれることが可能になり、安全性が強化されている．

【００４１】実施例２では，有限体上の離散対数問題と楕円曲線上の離散対数問題の２つを統合した鍵共有方式となっているが，実施例はこれに限定されない．例えば、有限体上の離散対数問題，楕円曲線上の離散対数問題の安全性の異なる２つ以上の方式を独立に対等に統合することにより，安全性を強化することも含まれる．

【００４２】

【発明の効果】以上に説明したように本発明は，従来例における問題点，すなわち従来の暗号方式，鍵共有方式，署名方式では，安全性の根拠を離散対数問題や素因数分解という一つの問題に帰着させているため，安全性を帰着している問題が攻撃された場合，その方式で構成されたすべてのデータが攻撃されることになる．すなわち、攻撃に対する頑強性を持たない。特に、鍵共有方式においては、従来例２で見たように、ユーザ間で同じシステムパラメータを用いて公開鍵、秘密鍵のペアを生成する必要があり、汎用性が損なわれるという問題があった。

【００４３】本発明は，この従来例における問題点を鑑みて行なわれたもので，独立な安全性をもつ問題を互いの安全性が独立であるように統合し，一つの問題が攻撃されても耐用可能な鍵共有，暗号，署名方法を提供することを目的とする．特に、鍵共有においては、ユーザが自由にシステムパラメータを設定することを可能にし、汎用性と利便性を実現した鍵共有，暗号，署名方法を提供することを目的にする。安全で汎用的な暗号方式、鍵共有方式、署名方式を提供することができ，その実用的価値は大きい．

【図面の簡単な説明】

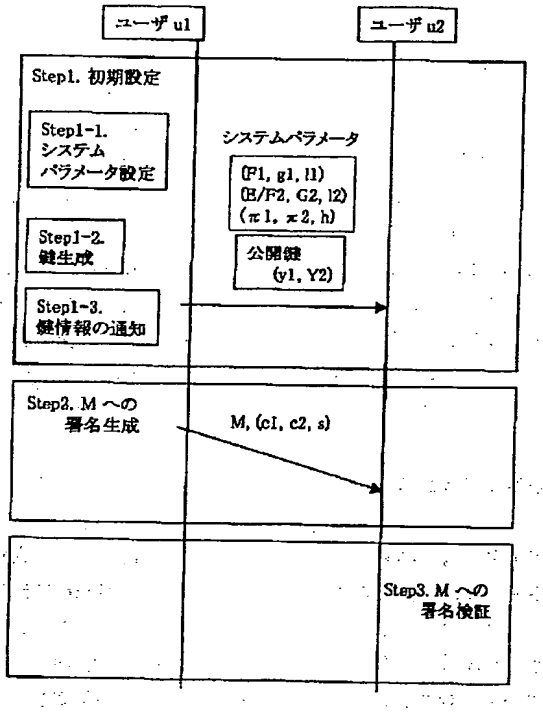
【図１】実施例１の署名装置の構成図

【図２】実施例２の鍵共有装置の構成図

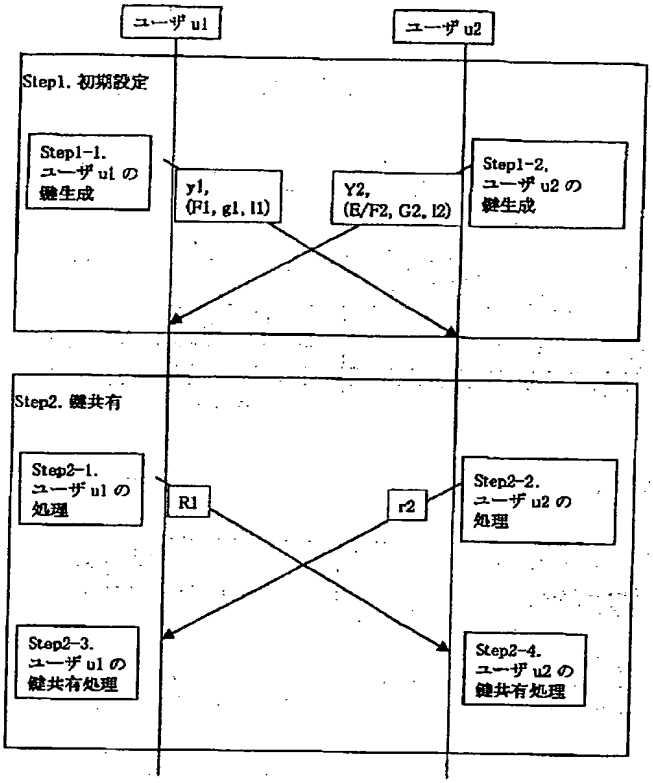
【図３】従来例１の楕円曲線上のＤＳＡ署名の構成図

【図４】従来例２の有限体上の鍵共有装置の構成図．

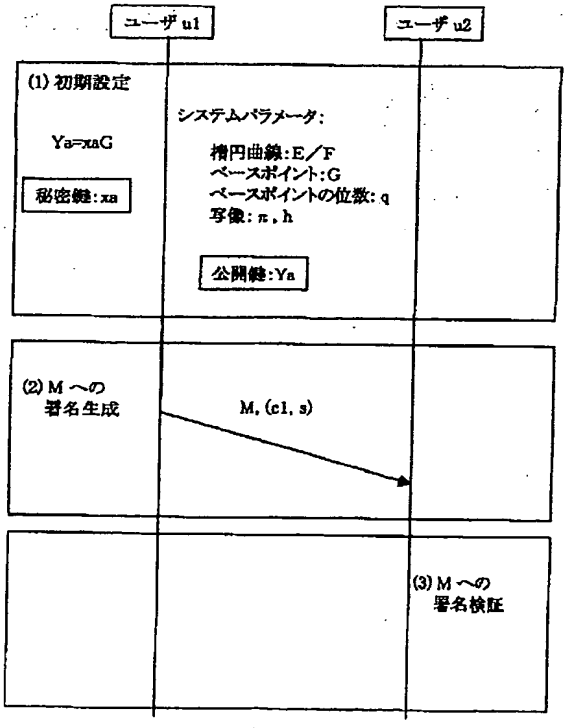
【図１】


ユーザ u1
ユーザ u2
Step1. 初期設定
Step1-1.
システム
パラメータ設定
システムパラメータ
(F1, g1, l1)
(E/F2, G2, l2)
(π1, π2, h)
Step1-2.
鍵生成
公開鍵
(y1, Y2)
Step1-3.
鍵情報の通知
Step2. M への
署名生成
M, (c1, c2, s)
Step3. M への
署名検証

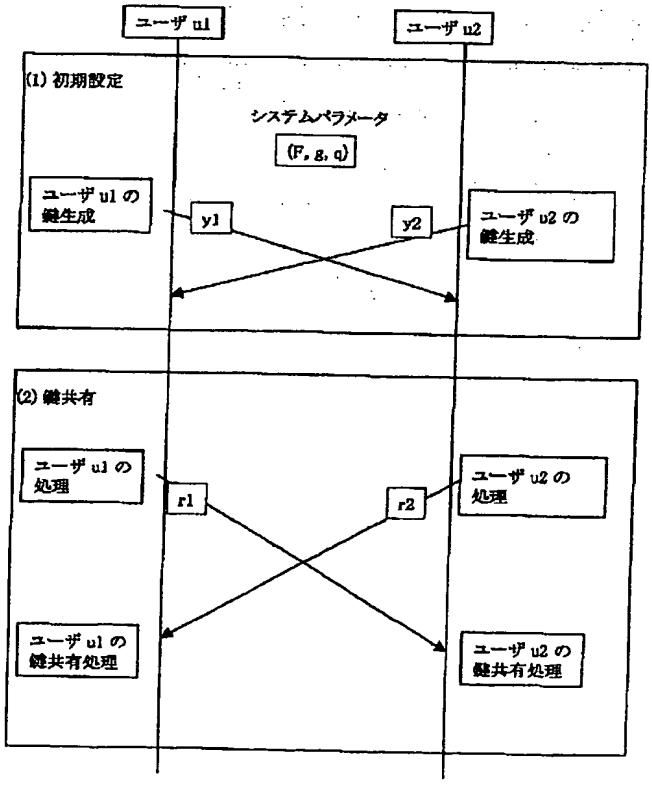
【図２】


ユーザ u1
ユーザ u2
Step1. 初期設定
Step1-1.
ユーザ u1 の
鍵生成
y1,
(F1, g1, l1)
Y2,
(E/F2, G2, l2)
Step1-2.
ユーザ u2 の
鍵生成
Step2. 鍵共有
Step2-1.
ユーザ u1 の
処理
R1
r2
Step2-2.
ユーザ u2 の
処理
Step2-3.
ユーザ u1 の
鍵共有処理
Step2-4.
ユーザ u2 の
鍵共有処理

【図３】


ユーザ u1
ユーザ u2
(1) 初期設定
Ya=xaG
秘密鍵:xa
システムパラメータ:
楕円曲線:E／F
ベースポイント:G
ベースポイントの位数: q
写像: π, h
公開鍵:Ya
(2) M への
署名生成
M, (c1, s)
(3) M への
署名検証

【図４】


ユーザ u1
ユーザ u2
(1) 初期設定
システムパラメータ
(F, g, q)
ユーザ u1 の
鍵生成
y1
y2
ユーザ u2 の
鍵生成
(2) 鍵共有
ユーザ u1 の
処理
r1
r2
ユーザ u2 の
処理
ユーザ u1 の
鍵共有処理
ユーザ u2 の
鍵共有処理

フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
		H04L 9/00	601E